Please type a plus sign (+) inside this box → ☐

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	CIS-044	Total Pages	31

First Named Inventor or Application Identifier

McCloghrie, Keith

Express Mail Label No.	EI924751370US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☐ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification   [*Total Pages* **26**]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (*if filed*)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. ☒ Drawing(s) *(35 USC 113)*   [*Total Sheets* **3**]

4. Oath or Declaration   [*Total Pages* ___]
   a. ☐ Newly executed (original or copy)
   b. ☐ Copy from a prior application (37 CFR 1.63(d))
   (for continuation/divisional with Box 17 completed)
   [Note Box 5 below]
   i. ☐ DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. ☐ Incorporation By Reference *(useable if Box 4b is checked)*
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ☐ Microfiche Computer Program *(Appendix)*

7. Nucleotide and/or Amino Acid Sequence Submission
(*if applicable, all necessary*)
   a. ☐ Computer Readable Copy
   b. ☐ Paper Copy (identical to computer copy)
   c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☐ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(b) Statement   ☐ Power of Attorney
(when there is an assignee)
10. ☐ English Translation Document *(if applicable)*
11. ☐ Information Disclosure Statement (IDS)/PTO-1449   ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. ☐ Small Entity Statement(s)   ☐ Statement filed in prior application, Status still proper and desired
15. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. ☒ Other: *Certificate of Mailing*

17. If a CONTINUING APPLICATION, *check appropriate box and supply the requisite information:*

☐ Continuation   ☐ Divisional   ☐ Continuation-in-part (CIP)   of prior application No: _____/_____

18. CORRESPONDENCE ADDRESS

☐ Customer Number or Bar Code Label
(Insert Customer No. or Attach bar code label here)   or ☒ Correspondence address below

NAME	Steven A. Swernofsky
	The Law Offices of Steven A. Swernofsky
ADDRESS	Post Office Box 390013
	Reg. No. 33,040
CITY	Mountain View	STATE	CA	ZIP CODE	94039-0013
COUNTRY	USA	TELEPHONE	(650) 947-0700	FAX	(650) 947-8438

1   This application is submitted in the name of the following inventors:

2

3   <u>Inventor</u>   <u>Citizenship</u>   <u>Residence City and State</u>

4   McCloghrie, Keith   United Kingdom   San Jose, California

5   Robert, Stephan   Switzerland   Neuchatel, Switzerland

6   Walrand, Jean   Belgium   Berkeley, California

7   Bierman, Andrew

8

9   The assignee is <u>Cisco Technology, Inc.</u>, a California corporation having an

10 office at 170 West Tasman Drive, San Jose CA 95134.

11

12 <u>Title of the Invention</u>

13

14 Sampling Packets for Network Monitoring

15

16 <u>Background of the Invention</u>

17

18 *1.   Field of the Invention*

19

20 This invention relates to network monitoring.

21

22 / / /

1   *2.   Related Art*

2

3   In a computer network in which messages are transmitted and received be-

4   tween devices, it is often desirable to monitor the nature and volume of communication

5   traffic. For example, by noting the number of messages (or more detailed information

6   about those messages) transmitted from selected source devices or to selected destination

7   devices, it can be possible to obtain useful information about usage patterns of the net-

8   work. One known set of network objects used for this purpose is called RMON ("remote

9   monitoring"). In known systems, a device coupled to and monitoring a communication

10   link in the network generates these RMON objects. RMON objects are retrievable from

11   the generating device using a known message protocol, such as SNMP (Simple Network

12   Message Protocol).

13

14   RMON was originally conceived for monitoring OSI layer 1 and layer 2

15   communication. Accordingly, a first version of RMON (RMON1) was directed to col-

16   lecting information and statistics primarily about packets between a source device MAC

17   address and a destination device MAC address. A first version of RMON1 was optimized

18   in some respects for Ethernet LAN communication; a second version was optimized for

19   token-ring LAN communication. RMON1 also included capabilities for capturing the

20   contents of selected packets, and for setting alarms upon selected events (those events

21   being distinguished for layer 1 and layer 2 communication).

22

1   A more recent version of RMON (RMON2) extends the monitoring capa-

2   bilities to include more analysis of actual packets, including identifying layer 3, layer 4,

3   and some application aspects of communication. For example, RMON2 includes capa-

4   bilities for collecting information about usage of particular routing protocols (such as IP

5   or IPX) and particular ports used at the source device or destination device (such as ports

6   for FTP or HTTP transactions). RMON2 also differs from RMON1 in the number of

7   communication links that are monitored by a single device.

8

9   In parallel with the evolution from RMON1 to RMON2, another evolution

10   has taken place: early RMON applications using RMON1 were usually directed to moni-

11   toring probes, which monitor a single port of a switch. More recent RMON applications

12   using RMON2 are often directed to monitoring software that is embedded in a switch,

13   and therefore is contemplated to monitor several, preferably all, interfaces of the switch.

14

15   One problem in the known art is that ability to monitor network traffic is

16   not keeping up with the amount and speed of the network traffic itself. First, more recent

17   versions of RMON result in an increase in the processing required for each packet. Sec-

18   ond, it is desirable to monitor as many output interfaces as possible. Third, the bandwidth

19   and wire speed of network interfaces is rapidly increasing due to advances in technology.

20   All three of these effects require additional processing power in the monitoring device.

21

1   One response to this problem is to select only a sample set of packets for

2   monitoring, rather than attempting to process all packets transmitted over the monitored

3   communication links. The sampled traffic would serve as a proxy for all traffic, to meas-

4   ure the frequency of selected network events and to collect aggregate information about

5   network traffic. United States Patent No. 5,315,580, titled "Network Monitoring Device

6   and System", issued May 24, 1994, in the name of Peter Phaal, to assignee Hewlett-

7   Packard Company of Palo Alto, California, shows one example of a sampling technique

8   for monitoring.

9

10   Known sampling techniques achieve the purpose of collecting aggregate

11   information about network traffic where the network transmission rate of packets exceeds

12   the ability of the monitoring device to process those packets. However, these techniques

13   suffer from several drawbacks. First, estimated frequency measurement for relatively in-

14   frequent events can be subject to error and inaccuracy. Second, processor load for the

15   monitoring device can vary wildly in response to network traffic load. When network

16   traffic is relatively frequent, processor load is relatively heavy, and the monitoring device

17   can fail to keep up with the network traffic. When network traffic is relatively infrequent,

18   processor load is relatively light, and the monitoring device can be underused.

19

20   Accordingly, it would be advantageous to provide a method and system for

21   collecting aggregate information about network traffic, in which processor load is rela-

22   tively constant despite substantial variation in network traffic, and in which the accuracy

1   of frequency measurement can be improved even for relatively infrequent events, due to

2   the ability to sample more frequently. This advantage is achieved in an embodiment of

3   the invention that samples packets from network traffic adaptively in response to that

4   network traffic, and measures frequency in response to either the sampling rate or the fre-

5   quency rate of appearance in sampled packets, or both.

6

7   Summary of the Invention

8

9   The invention provides a method and system for collecting aggregate in-

10   formation about network traffic, while maintaining processor load relatively constant de-

11   spite substantial variation in network traffic, and capable of substantially accurate fre-

12   quency measurement even for relatively infrequent events. A packet monitoring system

13   includes an input port for receiving network packets, a sampling element for selecting a

14   fraction of those packets for review, and a queue of selected packets. The packets in the

15   queue are coupled to a packet-type detector for detecting packets of a selected type; the

16   system applies a measurement technique for determining a frequency measure for those

17   detected packets. The system includes a feedback technique for adaptively altering the

18   sampling rate fraction, responsive to the queue length and possibly other factors, such as

19   processor load or the detected frequency measure.

20

21   In a preferred embodiment, the measurement technique also determines an

22   error range and a measure of confidence that the actual frequency is within the error range

1   of the measured frequency. The system can detect packets of multiple selected types, and

2   provide measured frequencies and error ranges for all of the multiple selected types con-

3   currently. Also, the measurement technique is selected so as to impose relatively little

4   computational load per packet.

5

6   Brief Description of the Drawings

7

8   Figure 1 shows a block diagram of a system for collecting information

9   about packet traffic.

10

11   Figure 2 shows a block diagram of a system for adaptively sampling pack-

12   ets.

13

14   Figure 3 shows a process flow diagram of a method for adaptively sampling

15   packets and measuring expected frequencies for selected packet types.

16

17   Detailed Description of the Preferred Embodiment

18

19   In the following description, a preferred embodiment of the invention is de-

20   scribed with regard to preferred process steps and data structures. Those skilled in the art

21   would recognize after perusal of this application that embodiments of the invention can

22   be implemented using circuits adapted to particular process steps and data structures de-

1   scribed herein, and that implementation of the process steps and data structures described

2   herein would not require undue experimentation or further invention.

3

4   *Sampling System Elements*

5

6   Figure 1 shows a block diagram of a system for collecting information

7   about packet traffic.

8

9   A system 100 for collecting information about packet traffic includes a

10   packet router or packet switch 110, a traffic management element 120, and a traffic in-

11   formation database 130.

12

13   The packet switch 110 includes a plurality of input interfaces 111 and out-

14   put interfaces 112. The packet switch 110 it is disposed to receive a sequence of packets

15   113 at one or more of those input interfaces 111, and to output those packets 113 (possi-

16   bly altered according to known packet rewrite rules) at one or more of those output inter-

17   faces 112. Packet routers and packet switches 110 are known in the art of computer net-

18   works.

19

20   The traffic management element 120 is coupled to at least one of the input

21   interfaces 111 or output interfaces 112. (In a the preferred embodiment, the traffic man-

22   agement element 120 is coupled to substantially all of the input interfaces 111 and to sub-

1   stantially all of the output interfaces 112.) The traffic management element 120 is dis-

2   posed to receive substantially all of the packets 113 input to the packet switch 110 and to

3   sample a fraction of those packets 113. Similarly, the traffic management element 120 is

4   also disposed to review substantially all of the packets 113 about to be output from the

5   packet switch 110 and to sample a fraction of those packets 113.

6

7   In alternative preferred embodiments, the traffic management element 120

8   can be distributed within a plurality of devices, such that sampling of packets 113 occurs

9   at the input interfaces 111 or output interfaces 112, while counting and analysis occur at

10   another logical location. In such alternative preferred embodiments, the portion of the

11   traffic management element 120 that actually samples input packets 113 marks each sam-

12   pled input packet 113 as a sample and forwards those sampled input packets 113 to an-

13   other portion of the traffic management element 120 for counting and analysis. Similarly,

14   the portion of the traffic management element 120 that actually samples output packets

15   113 marks each sampled output packet 113 as a sample, and forwards those sampled out-

16   put packets 113 back to the traffic management element 120. Sampling and forwarding

17   of output packets 113 does not actually output a duplicate packet 113 at the output inter-

18   face 112.

19

20   Since it is advantageous for the traffic management element 120 to perform

21   accurate counting and analysis, each sampled packet 113 (whether a sampled input packet

22   113 or a sampled output packet 113) thus forwarded is labeled with a sequence number.

1   This allows the portion of the traffic management element 120 performing counting and

2   analysis to avoid losing synchronization even if a sampled packet 113 is dropped after

3   forwarding by the portion of the traffic management element 120 for sampling and for-

4   warding.

5

6   The traffic management element 120 is coupled to the traffic information

7   database 130. The traffic management element 120 is disposed to output the information

8   it collects about sampled packets 113 to the traffic information database 130. The traffic

9   information database 130 is disposed to store that information and to output or present

10   that information in response to a request message 131 from a device coupled to the net-

11   work (not shown).

12

13   In a preferred embodiment, the traffic information database 130 records the

14   information about sampled packets 113 in a known format, such as the RMON MIB for-

15   mat, and the device coupled to the network communicates with the traffic information

16   database 130 using a known protocol such as the SNMP protocol. The RMON MIB for-

17   mat and the SNMP protocol are known in the art of computer networks.

18

19   *Adaptive Sampling System*

20

21   Figure 2 shows a block diagram of a system for adaptively sampling pack-

22   ets.

1

2   A system 200 for adaptively sampling packets includes a packet input port

3 210, a sampling element 220, a sampled packet queue 230, an adaptive sampling control-

4 ler 240, a sampled-packet output port 250, at least one packet type detector 260, and at

5 least one frequency measure element 270.

6

7   The packet input port 210 is disposed within the traffic management ele-

8 ment 120, and is disposed to receive substantially all of the packets 113 input to the

9 packet switch 110. In those alternative embodiment where the traffic management ele-

10 ment 120 is distributed in both a first portion for sampling and forwarding and a second

11 portion for counting and analysis, the packet input port 210 is disposed within the first

12 portion for sampling and forwarding.

13

14   In alternative embodiments, the packet input port 210 may be disposed to

15 receive only a selected subset of the packets 113 input to the packet switch 110, such as

16 only those packets 113 using a selected protocol such as IP or a selected protocol at an-

17 other layer such as HTTP. In further or other alternative embodiments, the packet input

18 port 210 may be disposed to receive packets 113 output by (rather than input to) the

19 packet switch 110.

20

21   The sampling element 220 is coupled to the packet input port 210 and is

22 disposed to sample one out of every N packets 113, where N is a control parameter. The

1   adaptive sampling controller 240 sets the value of N. In a preferred embodiment, the

2   value of N is adjusted to start at a default value, and adaptively adjusted thereafter, as de-

3   scribed herein. Thus, one out of every N packets is selected by the sampling element 220

4   for further processing by the traffic management element 120. In a preferred embodi-

5   ment, the default value of N is selected in response to the bandwidth of the packet input

6   port. For example, the default value can be set to 400 for a 1 gigabit-per-second port, 40

7   for a 100 megabit-per-second port, or 4 for a 10 megabit-per-second port.

8

9   The system 200 appends those packets 113 selected by the sampling ele-

10   ment 220 to the tail of the sampled packet queue 230. The sampled packet queue 230 is

11   disposed to receive, store, and present packets 113 in a FIFO (first in first out) manner.

12   FIFO queues are known in the art of computer programming. In a preferred embodiment,

13   the sampled packet queue 230 stores only pointers to packets 113, or pointers to packet

14   headers, and the original packets 113 or packet headers are stored in a memory. How-

15   ever, the operation of the system for adaptively sampling packets is substantially similar

16   regardless of whether the sampled packet queue 230 holds packets 113, packet headers,

17   pointers thereto, or some related data structure.

18

19   The sampled packet queue 230 is coupled to the adaptive sampling con-

20   troller 240. The adaptive sampling controller 240 compares the length of the sampled

21   packet queue 230 against a lower threshold 231 and an upper threshold 232. The adaptive

1   sampling controller 240 sets the value of the control parameter N responsive to this com-

2   parison, and outputs the value of N to the sampling element 220.

3

4   In a preferred embodiment, if the length is less than the lower threshold

5   231, the adaptive sampling controller 240 decreases the value of the control parameter N

6   (to sample more frequently). If the length is more than the upper threshold 232, the

7   adaptive sampling controller 240 increases the value of the control parameter N (to sam-

8   ple less frequently). Methods used by the adaptive sampling controller 240 are further

9   described with regard to figure 3. However, in alternative embodiments, the adaptive

10   sampling controller 240 may set the value of N responsive to other factors, including any

11   of the following (or some combination thereof):

12

13   o   the actual length of the sampled packet queue 230;

14

15   o   an average length of the sampled packet queue 230 for some recent time period, or

16   some other statistical parameter for that length, such as a maximum, minimum,

17   median, or variance thereof;

18

19   o   an average number of sampled packets 113 received at the sampled packet queue

20   230 for some recent time period, or some other statistical parameter for that num-

21   ber, such as a maximum, minimum, median, or variance thereof;

22

o   comparison of the actual or average length of the sampled packet queue 230, or the number of sampled packets 113 received at the sampled packet queue 230, with a further lower threshold (other than the lower threshold 231) or a further upper threshold (other than the upper threshold 232);

o   the presence (or absence) of a packet 113 of a selected particular type (such as a special flag packet 113, a packet 113 using a known protocol such as FTP, or a multicast packet 113) received at the sampled packet queue 230, or present in the sampled packet queue 230, for some recent time period.

In a preferred embodiment, the adaptive sampling controller 240 described herein is disposed to prevent processor overloading of the traffic management element 120, by sampling at a relatively less frequent rate when packets 113 are arriving relatively more often. However, in alternative embodiments, the adaptive sampling controller 240 may be disposed for other and further purposes, such as the following:

o   to obtain a more accurate count of selected particular types of packets;

o   to specifically respond to expected types of network traffic (such as network traffic that is expected to be relatively bursty or relatively sparse); or

1   o   otherwise to adapt to either the frequency or type of packets 113 seen by the traffic

2   management element 120.

3

4   These alternative embodiments would be clear to those skilled in the art af-

5   ter perusing this application, would not require undue experiment or further invention,

6   and are within the scope and spirit of the invention.

7

8   The sampled-packet output port 250 is coupled to the head of the sampled

9   packet queue 230. The sampled-packet output port 250 couples the sampled packets 113

10   to one or more packet type detectors 260.

11

12   In a preferred embodiment, there is a plurality of packet type detectors 260,

13   one for each of the selected packet types for which a frequency measurement is desired.

14   Each packet type detector 260 counts the number of sampled packets 113 that have the

15   selected packet type, of all those sampled packets 113 that are received. The total number

16   of sampled packets 113 which are received is also counted, either at each packet type de-

17   tector 260 or at a "universal" packet type detector 260, which counts all sampled packets

18   113.

19

20   Each packet type detector 260 is coupled to a corresponding frequency

21   measure element 270, which determines an expected frequency of the selected packet

22   type for all packets 113 in the network traffic, in response to the actual frequency of the

1   selected packet type for all sampled packets 113. Measurement techniques used by the

2   frequency measure elements 270 are further described with reference to figure 3.

3

4   Figure 3 shows a process flow diagram of a method for adaptively sampling

5   packets and measuring expected frequencies for selected packet types.

6

7   A method 300 for adaptively sampling packets and measuring expected fre-

8   quencies for selected packet types includes a set of flow points and process steps as de-

9   scribed herein. In a preferred embodiment, the traffic management element 120 (particu-

10   larly the adaptive sampling controller 240 and the frequency measure elements 270) per-

11   forms the method 300.

12

13   At a flow point 310, the traffic management element 120 is ready to receive

14   a sequence (or a continuation of a sequence) of packets 113.

15

16   At a step 311, the traffic management element 120 sets the control parame-

17   ter N (further described with regard to figure 2) to a preferred value of about N_0, further

18   described below, although values of N varying substantially from N_0 are also within the

19   scope and spirit of the invention.

20

1　　　　　At a step 312, the traffic management element 120 receives a sequence of

2　packets 113 and samples 1 out of N of those packets 113 using the sampling element 220

3　to provide a stream of sampled packets 113.

4

5　　　　　At a step 313, the traffic management element 120 queues the stream of

6　sampled packets 113 using the sampled packet queue 230, and counts the actual number

7　of packets of each selected type using the packet type detectors 260.

8

9　　　　　At a step 314, the traffic management element 120 compares the length of

10　the sampled packet queue 230 with the lower threshold 231 and with the upper threshold

11　232. In a preferred embodiment, the lower threshold 231 is constant and substantially

12　equals a control parameter A. The traffic management element 120 performs a step 315,

13　a step 316, or a step 317, in response to the comparison, and continues with the step 312.

14

15　　　　　If the length is less than the lower threshold 231, the traffic management

16　element 120 performs the step 315. At the step 315, the traffic management element 120

17　uses the adaptive sampling controller 240 to increase the value of the control parameter N

18　by a factor of α, where α is a control parameter. The new control parameter N is main-

19　tained for at least S new sample packets 113, where S is a control parameter.

20

21　　　　　If the length is between the lower threshold 231 and the upper threshold

22　232, the traffic management element 120 performs the step 316. In a preferred embodi-

1 ment, the upper threshold 232 is constant and substantially equals a control parameter B.

2 At the step 316, does not adjust the control parameter N.

3

4 If the length is more than the upper threshold 232, the traffic management

5 element 120 performs the step 317. At the step 317, the traffic management element 120

6 uses the adaptive sampling controller 240 to decrease the value of the control parameter N

7 by a factor of β, where β is a control parameter. The new control parameter N is main-

8 tained for at least S new sample packets 113, where S is the control parameter described

9 above.

10

11 In a preferred embodiment, the following values of the control parameters

12 are used.

13

14 N_0 about 400   (as described above)

15 A   about 15

16 α about 2

17 B   about 30

18 β about 2

19 S   about 10

20

21 The inventors have found by simulation that these values of the control pa-

22 rameters do not produce skew.

17

1

2   However, in alternative embodiments, substantially different values for

3 these control parameters may be used; such alternative embodiments would not require

4 undue experiment or further invention, and are within the scope and spirit of the inven-

5 tion.

6

7   At a flow point 320, the traffic management element 120 is ready to com-

8 pute a frequency measure of packets 113 of a selected particular type.

9

10   In a preferred embodiment, the steps following the flow point 310 are per-

11 formed in parallel with the steps following the flow point 320. Thus, operation of the

12 sampling element 220 and the adaptive sampling controller 240 (to sample packets 113) is

13 in parallel with operation of the packet type detectors 260 and their corresponding fre-

14 quency measure elements 270 (to compute the frequency measure of packets 113 of each

15 selected particular type).

16

17   At a step 321, the packet type detector 260 for a first selected type K detects

18 a packet 113 of that type K.

19

20   At a step 322, the corresponding frequency measure element 270 for the

21 first selected type K updates its counts of the estimated number of packets 113 of type K,

1 and of the actual number of total packets 113. In a preferred embodiment, the following

2 information is maintained:

3

4 O   *count*   the estimated number of packets of type K

5 O   *variance*   the estimated variance of the count

6 O   *i*   the number of packets

7 O   *j*   the value of *i* for the last sampled packet of type K

8 O   *n*   the number of sampled packets

9 O   *m*   the value of *n* for the last sampled packet of type K

10

11 At a step 323, the frequency measure element 270 for the first selected type

12 K determines an estimated count (from which an average frequency can be computed) for

13 packets 113 of the selected type K, and a variance for the estimated count of packets 113

14 of the selected type K, according to the following sub-steps:

15

16 At a sub-step 323(a), a temporary value N_{temp} is set equal to an estimated

17 number of packets of type K which have passed by between this sampled packet of type K

18 and the most recent previously sampled packet of type K. In a preferred embodiment,

19 N_{temp} is set equal to $(i - j) / (n - m)$.

20

21 At a sub-step 323(b), the estimated number of packets of type K is updated.

22 In a preferred embodiment, *count* is set equal to *count* $+ N_{temp}$.

1

2   At a sub-step 323(c), the estimated variance is updated. In a preferred em-

3   bodiment, if $m < (n - 1)$ then *variance* is set equal to *variance* + 2 N_{temp}.

4

5   At a sub-step 323(d), the counts j and m are updated. In a preferred em-

6   bodiment, m is set equal to n, and i is set equal to j.

7

8   In a preferred embodiment, the best estimate of the count is *count*, and the

9   best estimate of the 95% confidence interval is given by *count* $\pm$ 2 **sqrt** (*variance*) where

10   **sqrt** is a square root function.

11

12   *Alternative Embodiments*

13

14   Although preferred embodiments are disclosed herein, many variations are

15   possible which remain within the concept, scope, and spirit of the invention, and these

16   variations would become clear to those skilled in the art after perusal of this application.

Claims

1

2

3   1.   A method including steps for collecting aggregate information about

4   network traffic while maintaining processor load relatively constant despite substantial

5   variation in network traffic.

6

7   2.   A system including

8   means for collecting aggregate information about network traffic; and

9   means for maintaining processor load relatively constant for said means for

10   collecting despite substantial variation in network traffic.

11

12   3.   A system, including

13   an input port for receiving network packets;

14   a sampling element for selecting a fraction of those packets for review, said

15   sampling element including a feedback element for adaptively altering said fraction;

16   a queue of selected packets;

17   a packet-type detector coupled to said queue; and

18   a frequency measurement element coupled to said packet-type detector.

19

20   4.   A system as in claim 3, wherein said feedback element is responsive

21   to a length of said queue.

22

1   5.   A system as in claim 3, wherein said feedback element is responsive

2   to a load on said frequency measurement element.

3

4   6.   A system as in claim 3, wherein said feedback element is responsive

5   to a frequency measure determined by said frequency measurement element.

6

7   7.   A method, including steps for sampling a set of packets at a network

8   interface of a switch, said steps for sampling including steps for adaptively altering a

9   fraction of said packets for selection.

10

11   8.   A method as in claim 7, wherein said steps for adaptively altering a

12   fraction of said packets for selection include steps for

13   maintaining a queue of selected packets;

14   altering said fraction in response to a length of said queue.

15

16   9.   A method as in claim 7, wherein said steps for adaptively altering a

17   fraction of said packets for selection include steps for

18   measuring a frequency of packets of a known type within said selected

19   packets;

20   altering said fraction in response to a load imposed by said steps for meas-

21   uring.

22

1   10.   A method as in claim 7, wherein said steps for adaptively altering a

2   fraction of said packets for selection include steps for altering said fraction in response to

3   two or more factors responsive to said selected packets.

4

5   11.   A method as in claim 7, including steps for determining a frequency

6   of packets of a known type within said selected packets.

7

8   12.   A method as in claim 11, including steps for determining an error

9   range for said measured frequency.

10

11   13.   A method as in claim 11, including steps for

12   setting a control parameter;

13   sampling said received packets in response to said control parameter, to

14   provide a queue of sampled packets;

15   comparing a length of said queue with a threshold;

16   altering said control parameter in response to said threshold.

17

18   14.   A method as in claim 13, wherein said control parameter is a fraction

19   of said received packets to sample for said queue.

20

21   15.   A method as in claim 13, wherein said threshold includes at least one

22   of: a lower bound for said length, an upper bound for said length.

1

2   16.   A method as in claim 13, wherein said threshold includes a lower

3   bound for said length and said steps for altering said control parameter operate to

4   lengthen said queue in response to said steps for comparing.

5

6   17.   A method as in claim 13, wherein

7   said control parameter is a fraction of said received packets to sample for

8   said queue;

9   said threshold includes a lower bound for said length; and

10   said steps for altering said control parameter decrease said control parame-

11   ter in response to said steps for comparing.

12

13   18.   A method as in claim 13, wherein said threshold includes an upper

14   bound for said length and said steps for altering said control parameter operate to shorten

15   said queue in response to said steps for comparing.

16

17   19.   A method as in claim 13, wherein

18   said control parameter is a fraction of said received packets to sample for

19   said queue;

20   said threshold includes an upper bound for said length; and

21   said steps for altering said control parameter increase said control parameter

22   in response to said steps for comparing.
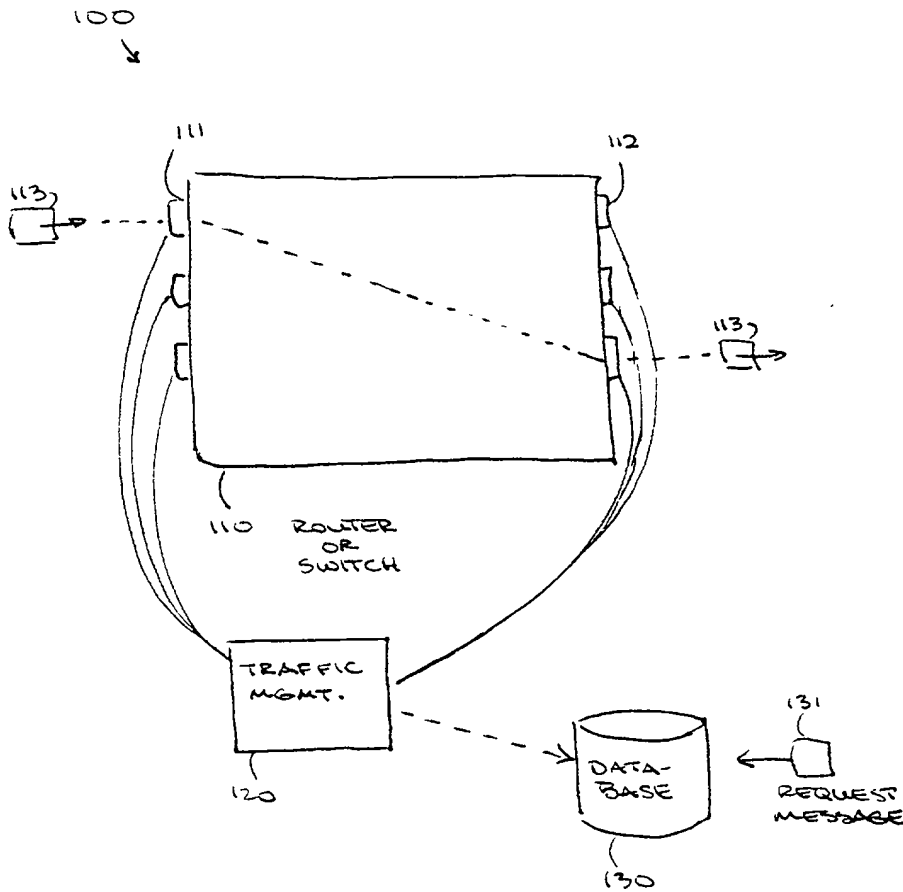
24

1

2   20.   A method as in claim 13, wherein said steps for altering said control

3 parameter operate to maintain said control parameter constant for at least a selected num-
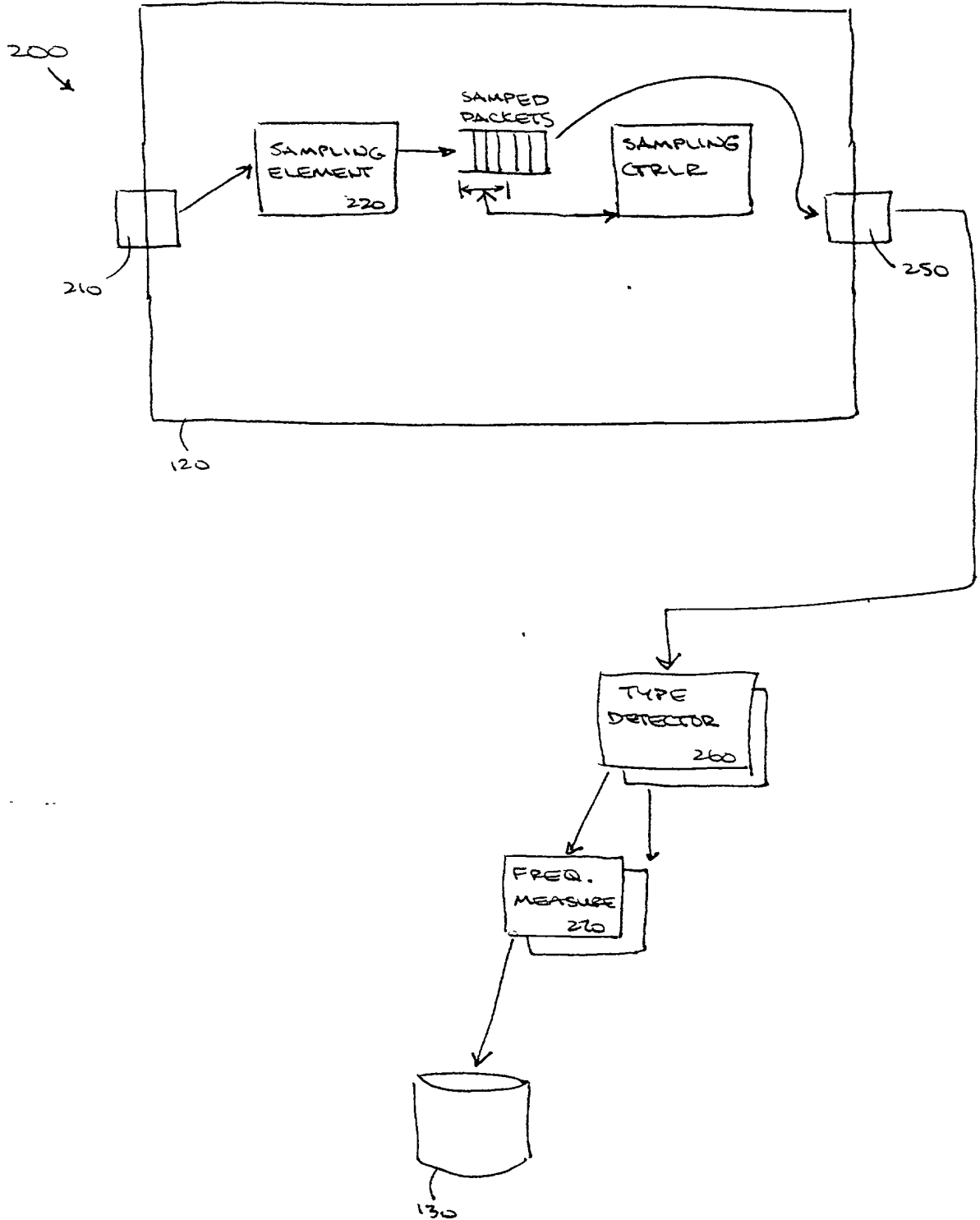
4 ber of sampled packets.

5

6   21.   A method as in claim 13, wherein said steps for sampling do not

7 produce skew.
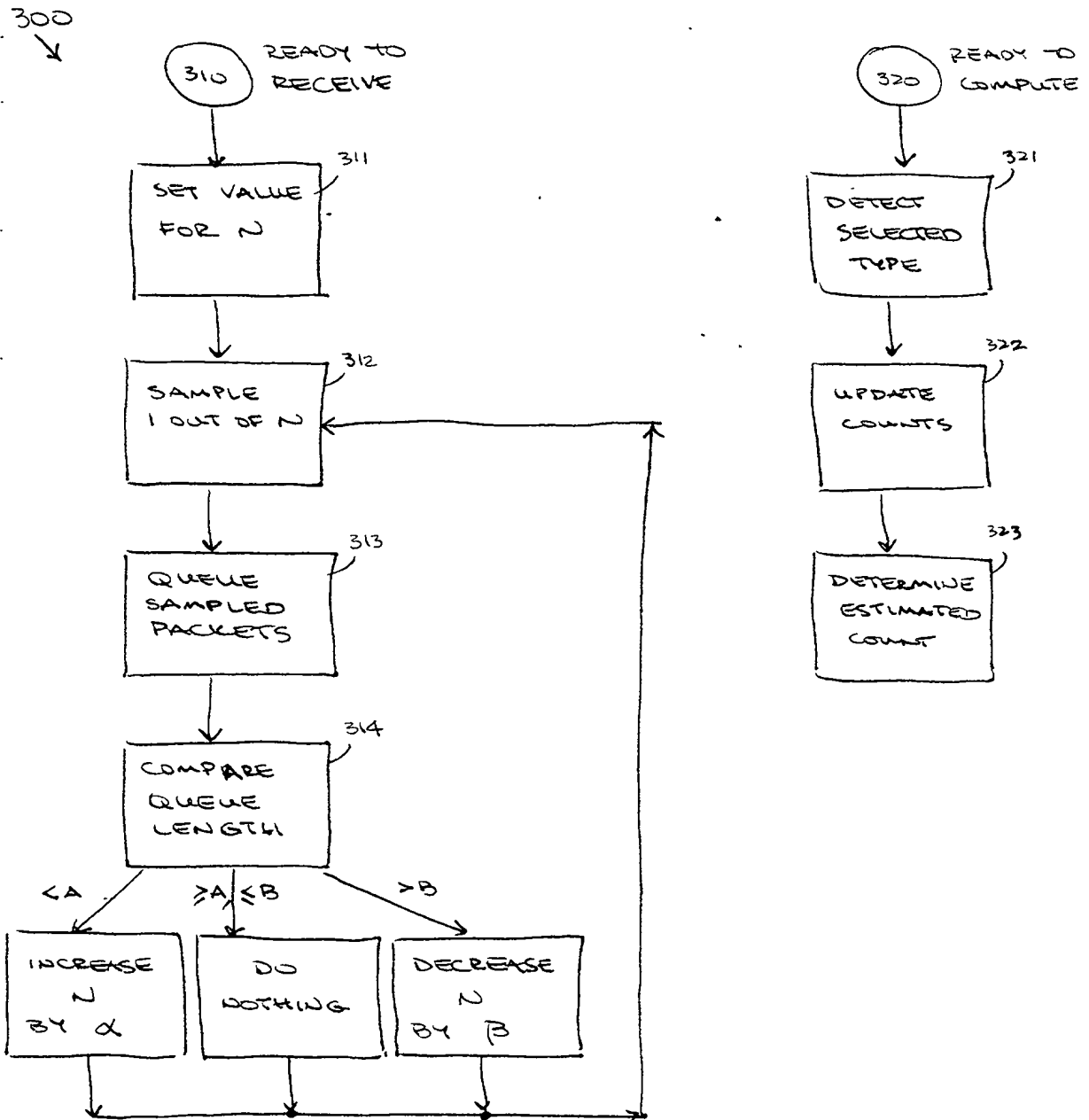
Abstract of the Disclosure

1

2

3 The invention provides a method and system for collecting aggregate in-

4 formation about network traffic, while maintaining processor load relatively constant de-

5 spite substantial variation in network traffic, and capable of substantially accurate fre-

6 quency measurement even for relatively infrequent events. A packet monitoring system

7 includes an input port for receiving network packets, a sampling element for selecting a

8 fraction of those packets for review, and a queue of selected packets. The packets in the

9 queue are coupled to a packet-type detector for detecting packets of a selected type; the

10 system applies a measurement technique for determining a frequency measure for those

11 detected packets. The system includes a feedback technique for adaptively altering the

12 sampling rate fraction, responsive to the queue length and possibly other factors, such as

13 processor load or the detected frequency measure. The measurement technique also de-

14 termines an error range and a measure of confidence that the actual frequency is within

15 the error range of the measured frequency. The system can detect packets of multiple se-

16 lected types essentially simultaneously, and provide measured frequencies and error

17 ranges for all of the multiple selected types at once. Also, the measurement technique is

18 selected so as to impose relatively light processor load per packet.

100

111   112

113

113

110   ROUTER
      OR
      SWITCH

TRAFFIC
MGMT.

120

131

DATA-
BASE

REQUEST
MESSAGE

130

CIS-044
FIGURE 1.

200

SAMPED PACKETS

SAMPLING ELEMENT 220

SAMPLING CTRLR

210

120

250

TYPE DETECTOR 260

FREQ. MEASURE 220

130

CIS-044
FIGURE 2.

300

310 READY TO RECEIVE

320 READY TO COMPUTE

311 SET VALUE FOR N

321 DETECT SELECTED TYPE

312 SAMPLE 1 OUT OF N

322 UPDATE COUNTS

313 QUEUE SAMPLED PACKETS

323 DETERMINE ESTIMATED COUNT

314 COMPARE QUEUE LENGTH
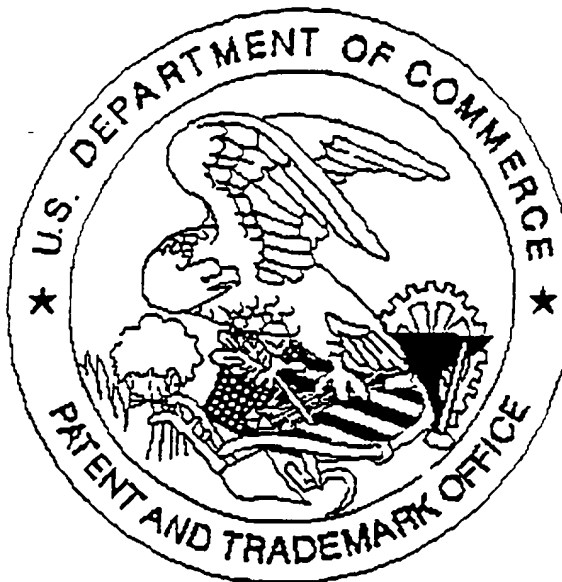
<A

≥A ≤B

>B

INCREASE N BY α

DO NOTHING

DECREASE N BY β

CIS-044
FIGURE 3.

United States Patent & Trademark Office
Office of Initial Patent Examination -- Scanning Division

Application deficiencies found during scanning:

1. Application papers are not suitable for scanning and are not in compliance with 37 CFR 1.52 because:
   - ☐ All sheets must be the same size and either A4 (21 cm x 29.7 cm) or 8-1/2"x 11"
     Pages _____ do not meet these requirements.
   - ☐ Papers are not flexible, strong, smooth, non-shiny, durable, and white.
   - ☐ Papers are not typewritten or mechanically printed in permanent ink on one side.
   - ☐ Papers contain improper margins. Each sheet must have a left margin of at least 2.5 cm (1") and top, bottom and right margins of at least 2.0 cm (3/4").
   - ☐ Papers contain hand lettering.

2. Drawings are not in compliance and were not scanned because:
   - ☐ The drawings or copy of drawings are not suitable for electronic reproduction.
   - ☐ All drawings sheets are not the same size. Pages must be either A4 (21 cm x 29.7 cm) or 8-1/2" x 11".
   - ☐ Each sheet must include a top and left margin of at least 2.5 cm (1"), a right margin of at least 1.5 cm (9/16") and a bottom margin of at least 1.0 cm (3/8").

3. Page(s)_____ are not of sufficient clarity, contrast and quality for electronic reproduction.

4. Page(s)_____ are missing.

5. OTHER: No Declaration _____